UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/690,017	10/21/2003	James P. Goddard	END920030107US1	4833

26502 7590 04/19/2007

IBM CORPORATION
IPLAW IQ0A/40-3
1701 NORTH STREET
ENDICOTT, NY 13760

EXAMINER	
HOANG, DANIEL L	
ART UNIT	**PAPER NUMBER**
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/690,017	GODDARD, JAMES P.	
	Examiner	Art Unit	
	Daniel L. Hoang	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 February 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3, 8-10,12,15,19,20 and 25-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 3, 8-10, 12, 15, 19-20, 25-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments with respect to amended claim 1 have been considered but are moot in view of the new ground(s) of rejection. The remaining new and amended claims are addressed below.

CLAIMS PRESENTED

Claims 1, 3, 7-10, 14-15, 19, and 25-37 are presented.

CLAIM REJECTIONS

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 12 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 12:

Claim 12 recites the limitation "determining whether there is an intrusion detection system and vulnerability scanning for said application" in lines 3-4. It is unclear to examiner whether an intrusion detection system and vulnerability scanning exists in said application or whether intrusion detection systems and vulnerability scanning are performed on the application. For purposes of examination, examiner interprets the claim as meaning the latter.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3, 15, 19-20, 29, 30-31, and 35-37

Claims 1, 7-10, 14, 25-29, and 32-34 are rejected under 35 U.S.C. 102(e) as being anticipated by Goldfeder et al, US PGP No. 20040230835, hereinafter Gold.

As per claim 1, 25, and 32, Gold teaches:

A computer implemented method for evaluating a security risk of an application, said method comprising the steps of:

determining whether the application is shared by different customers;

[see paragraph 3 wherein Gold defines spyware as a security threat comprising of software that is designed by software developers that contain overt functions such as recording information about the user that is later returned to a marketing entity.]

[see paragraph 18 wherein the system is configured to analyze the application to detect security risks such as spyware]

Examiner interprets the detection of spyware to be equivalent to determining whether the application is shared by different customers. The different customers being the user that installs said software as well as the software developers that also use the program to embed spyware.

determining whether a third party can have unauthorized administrative authority to data maintained by said application;

[see above wherein software developers utilize spyware to gain access to data that may only be access by authorized administrators.]

determining whether a third party can have unauthorized read and/or write access to data maintained by said application;

[see paragraph 22 wherein evaluation engine 242 may be configured to evaluate privacy concerns about the application. Examiner interprets privacy concerns to be privacy of data, including read and/or write access]

assigning a numerical value or weight to each of the foregoing determinations, each of said numerical values or weights corresponding to a significance of the respective determination in evaluating security risk; and

[see paragraph 23 wherein evaluation engine is configured to assess the application against its particular rules or criteria to determine a score]

combining said numerical values or weights to evaluate security risk.

[see paragraph 23 where the scores are aggregated into a score collection]

As per claim 7, 26, and 33, Gold teaches:

A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether a third party can have unauthorized read and write access to said data; and

assigning a numerical value or weight to the determination whether a third party can have unauthorized read and write access to said data, and using the numerical value or weight for the determination whether a third party can have unauthorized read and write access to said data in evaluating said security risk.

[see figure 4, wherein a user can view the score [element 405] and determine whether the application can have access or not using element 410]

As per claim 8 and 27, Gold teaches:

A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether a vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs; and

assigning a numerical value or weight to the determination whether the vulnerability in said application can be exploited by a person or program which has not been authenticated to said application or a system in which said application runs and using the numerical value or weight for the determination whether a third party can have unauthorized read and write access to said data in evaluating said security risk.

[see rejection of claim 1 wherein examiner interprets that the existence of spyware in an application is equivalent to a vulnerability in an application. Further, see rejection of claim 7 wherein the score is used to determine whether a third party can have read and write access.]

As per claim 9, Gold teaches:

A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether data maintained by or accessed by said application is confidential; and wherein the numerical value or weight assigned to the determination whether a third party can have unauthorized access to said data is based in part on whether said data is confidential.

[see rejection of claim 1, privacy of data, wherein examiner interprets private data as confidential data.]

As per claim 10, 28, and 34, Gold teaches:

A method as set forth in claim 1 further comprising the steps of:

determining whether a customer has direct use of said application; and assigning a numerical value or weight to the determination whether a customer has direct use of said application, and using the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk.

[see paragraph 2 wherein a computer user installs computer programs. It is clear that if the user installed the program, it is possible that the user has direct access to the installed program.]

[also see rejection of claim 7 wherein the score is used to determined the customer's right to access, which examiner interprets to encompass use of the application.]

As per claim 12, Gold teaches:

A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether there is an intrusion detection system and vulnerability scanning for said application; and assigning a numerical value or weight to the determination whether there is an intrusion detection system and vulnerability scanning for said application, and using the numerical value or weight for the determination whether a customer has direct use of said application in evaluating said security risk.

[see paragraph 3-4 wherein Gold discloses that anti-virus and anti-spyware utilities are well known in the art and that they operate separately from each other without knowledge of each other's results.]

[also see rejection of claim 7 wherein the score is used to determined the customer's right to access, which examiner interprets to encompass use of the application.]

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 15, 19-20, 29, 30-31, and 35-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goldfeder et al, US PGP No. 20040230835

As per claim 3, Gold teaches:

A computer implemented method as set forth in claim 1 further comprising the steps of:

determining whether said application is subject to industry controls for security; and assigning a numerical value or weight to the determination whether said application is subject to industry controls for security, and using the numerical value or weight for the determination whether said application is subject to industry controls for security in evaluation security risk.

> *[as disclosed in applicant's specification, industry controls exist and are well know. Further disclosed by applicant is existing standard, NIST 800-37 which is used for certifying applications. Being that Gold's invention relates to evaluating security risks associated with an application, it would be obvious to one of ordinary skill in the art to subject them said applications to industry controls]*

As per claim 15, 29, and 35:

A computer implemented method as set forth in claim 1 further comprising the steps:

determining whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems; and assigning a numerical value or weight to the determination

whether there is a requirement for authentication of said application or a system in which said application runs to other systems before connection of said application or said system in which said application runs to said other systems, and using the numerical value or weight for said requirement for authentication in evaluating said security risk.

[see rejection of claim 1 wherein privacy concerns could obviously be addressed by requiring the application to authenticate itself]

As per claim 19, 30, and 36:

A computer implemented method as set forth in claim 1 further comprising the step of comparing the evaluation of said security risk to a cost savings provided by said application, and determining whether to certify said application for use based in part on said comparison.

It would be obvious to one of ordinary skill in the art at the time of the invention to which the subject matter pertains to compare the cost effect of allowing or disallowing the application. If allowing the application to be used is more costly then blocking use of the application then it would be more cost advantageous to block the application. Depending on the organization implementing the system, cost could be a mitigating factor in determining whether or not to certify the application.

As per claim 20, 31, and 37,

A computer implemented method as set forth in claim 1 further comprising the step of comparing the evaluation of said security risk to a revenue provided by said application, and determining whether to certify said application for use based in part on said comparison.

[see rejection of claim 19, wherein costs clearly have an effect on revenue.]

CONCLUSION

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

*. Any response to this Office Action should be **faxed to** (571) 273-8300 **or mailed to**:

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Hand-delivered responses should be brought to

Customer Service Window
Randolph Building
401 Dulaney Street
Alexandria, VA 22314

*. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel L. Hoang whose telephone number is 571-270-1019. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached at (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel L. Hoang
4/11/07

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

4/12/07